ERICSSON

Reference: RINAT-16: 0040
Date: 2016-09-05
Attending to this matter: Sreenivasa Reddy

To
Advisor (QoS)
TRAI
Old Minto Road
New Delhi

Ericsson's Response to TRAI Consultation Paper on Cloud Computing

Dear Sir,

We thank TRAI for providing an opportunity to respond to the above consultation paper. Ericsson is pleased to submit its response. Ericsson supports and actively contributes to various inititives by Global standadardisation Bodies, Government, Regulators, Policy Makers and Industry for an open cloud environment, open platforms and interfaces of those that makes it possible to mix and match components in the cloud. Specially for Mobility, the ambition to virtualize Network Functions and use common equipment as far as possible creates new demands on the virtualization and SDN layer. These demands are fulfilled by creating a Real Time capable Cloud with characteristics to both run on common equipment as well as run on specific equipment where this is needed. There are possibilities to use common equipment NFV, but needs the right virtualization and SDN layer.

Cloud technologies bring unprecedented agility, efficiency and accessibility to IT environments in every industry. Forward-looking businesses are already transforming to capture these benefits and turn them into effective differentiators. Ericsson therefore sees cloud, along with broadband and mobility, as a key enabler of the Networked Society.

Digital industrialization

There is a new definition of industrialization brought by the explosion of data, advanced analytics, and new digital technologies. LTE, LTE-A, 5G, IoT and the full realization of the Networked Society through Mobility, Broadband and Cloud will accelerate this transition.

Connecting the next billion devices, storing petabytes of data, and achieving millisecond latency to support the new speed of business necessitates a fundamental shift. It's a continuous cycle that organizations are seeing their IT infrastructure not as a cost item but as an asset. Success in the digital industrialization era will be realized by the operators, service providers and global multi-national companies that gain a technological advantage by operationalizing a continual stream of digital innovations.

The progression of the Digital Economy towards the Networked Society by definition implies a continued fast-paced evolution of the relationship between data subjects

Ericsson India Pvt. Ltd.

Ericsson Forum
DLF Cyber Citi, Sector 25-A
Gurgaon 122 002, Haryana,
www.ericsson.co.in/

Tel: +91 124 270 1201
Fax: +91 124 256 5420

Registered Office
4th Floor, Dakha House
VAT: 18/17, W.E.A, Pusa
New Delhi 110 005 INDIA

Service Tax No.:
IV916)ST/GGN-/CE/18/2002
TIN: 06911822715

and data controllers as well as the continued evolution of the concept of personal data. This has a few important implications:

A certain, not necessarily constant, minimum level of end user trust and hence data protection and fair processing is a must to assure a smooth evolution towards the Networked Society. This term aims to capture the regulation of the relationship between data subjects and data controllers, a small set of key principles that promote an adequate level of end-user trust to stimulate a satisfactory continuation of the progression towards digitalisation.

This “retail-level” Cloud regulation has to be promoted in a context that accommodates a set of legitimate business needs, such as legal basis for lawful processing, definition of personal data, profiling, analytics etc., and in particular, a “**business and consumer friendly regulatory framework**” that stimulates innovation, industry growth and commercial freedom for businesses and consumer to decide how to organize, where to source and locate key value chain activities.

The Networked Society is, even to a greater extent a borderless global community; hence the reality of existing regional differences (cultural, political, religious, etc.) puts limits on the attainable global data protection policy/ regulatory harmonization. This is necessary to assure compliance with globally fragmented regulatory environments at reasonable cost for multinational businesses and to avoid the risk of increasing trade barriers related to trans-border data flows that would favor national/local players.

International harmonization efforts between nations and regions will open up, expand and simplify trans-border data flows. In order to avoid fragmentation of the desired harmonized legislation through differences in national application should deliver de-facto harmonized outcomes at these levels:

- Legal framework
- Regulatory instrument, including, clear legal definitions of key regulatory objects (such as personal data)
- Regulatory implementation strategy and
- Enforcement, including Governance principles.

It is requested that a regulatory framework that makes **purpose of use of personal data** as the key regulatory objective and does not focus on prescribing how data is collected and processed. Regulation should be neutral to the choice of technology and process for the collection and processing of the personal data as long as this is not used to circumvent the regulatory objectives. We request TRAI to support business model, technology and process neutral:

- Legal and regulatory framework,
- Choice of regulatory instruments,
- Implementation strategy of regulatory instruments.

A flexible approach in defining objects such as sensitive data, since this definition has strong national, historical and cultural connotations.

A flexible approach by promoting alternatives to top-down implementation strategies e.g. an active policy engagement for the development of co-regulation frameworks, industry code of conduct and company certifications. This can alleviate gaps in standards between existing national privacy laws as well as make formal top-down frameworks more flexible and able to cope with the fast-paced and dynamic development in the ICT field.

It is also envisaged that promotion of a more **accountability-seeking legal and regulatory framework** that incentivises and rewards organizations rather than merely seeks compliance.

Cloud drivers and challenges:

In the Networked Society, there are a number of drivers for Government and Enterprises moving to cloud. At the same time, there are challenges to overcome. Public Cloud usage has attained high importance in recent years, along with Private Clouds; however, the challenge remains as how to use them most effectively and efficiently using the benefits of economies of scale. There are advantages with today's public clouds such as service richness and scale, but also limitations when it comes to Geography, Legal Frameworks, Governance and Security.

Hybrid Clouds

Many organizations deploy applications across both private and public clouds. The reasons for a hybrid cloud environment are many and generally depend on workload, type of application and sensitivity of application. Understanding how to integrate legacy hardware, applications and data with the latest public and private clouds into one single, governed model is key, and this enables a Hybrid Cloud model with one consistent deployment and orchestration process. Long-term data sustainability depends upon Enterprises being able to deploy workloads wherever they need to, without making significant physical or policy compromises.

Data Sovereignty and Legal Frameworks

The current public clouds that have sufficient scale and strength; with mission critical applications are still extremely geographically limited and as such Clouds can only be used for hosting workloads with less sensitivity to sovereignty or latency. Legal frameworks often put requirements that data must be stored in-country. Earlier, the Safe Harbor Privacy Principles between US and EU and Switzerland enabled US public cloud providers to store data in the US, but this was ruled invalid in 2015 and is now substituted by the EU-US Privacy Shield. We would urge TRAI to advise the Government of India to explore the possibilities of joining or creating such privacy shield agreements with other nations under its sovereign rights to reap the benefits of privacy, security under cloud environment while enabling digital economy.

Virtualization

There is a trend towards “functionality” virtualization, in order to achieve flexibility and agility. For network operators, network functions virtualization (NFV) and software defined networks (SDN) are being deployed.

Virtualizing a system or component—such as a processor, memory, or an I/O device—at a given abstraction level maps its interface and visible resources onto the interface and resources of an underlying, possibly different, real system. Consequently, the real system appears as a different virtual system or even as multiple virtual systems. Unlike abstraction, virtualization does not necessarily aim to simplify or hide details.

What is the purpose of virtualization?

- Abstraction
- Replication
- Isolation

A virtual machine monitor or hypervisor manages the virtual machines.

Governance and security for mission critical workloads

Organizations and enterprises must take cautious decisions on where to store data. Public cloud is fine for many applications, while for more mission critical applications private clouds might be a preferred option. Requirement on latency is one major consideration, while security and governance concerns are other important aspects

Hyperscale

There are a few giant public cloud providers which have developed “Hyperscale” computing approaches and changed the rules of the game in datacenter design, construction and management. They have moved on from traditional IT practices around datacenter design, hardware procurement and lifecycle management and business operation. By having discipline and focus on issues of power, cooling, server, storage, network, automation and governance, these leading cloud providers have reached new levels of efficiency, performance and agility. This approach enables them to rapidly scale up or down, adapt and deliver highly focused and resilient customer-centric solutions, realize capex and opex reductions and gain speed, scalability and flexibility. **In order to be successful in cloud operations, hyperscale is the norm,** realized either in own datacenters or in partnership with hyperscale players.

The promise of cloud is big, and the expectations are many:

- Lower Total Cost of Ownership: The Total Cost of Ownership (TCO) will be lower by adopting a cloud model, compared to traditional data centers.

- Enabling new business models: One such business model is the creation of offering “X as-a-Service” (XaaS) which lowers entry barriers as well as enables economies of scale. This is an opportunity for operators as well as other enterprises.
- Increased flexibility: By virtualization of network functions, it is possible to be more agile and flexible and enables scaling up and down capacity depending on need.
- New revenue opportunities: By being able to quickly launch new services to market and also enable penetration of markets that were earlier not possible.
- Enabling productivity and efficiency gains: One of the main drivers for cloud adoption is that it will enable productivity and efficiency gains. In a recent Ericsson Consumer Lab study, IT decision makers were asked about their expected outcomes of moving to cloud and this aspect came out highest.

Operate with efficiency:

IT operations, regardless of industry, are under pressure to deliver speed, scalability and flexibility that business demands, while at the same time cutting down on capex and opex. By transforming to cloud infrastructure, organizations can improve the efficiency in their operations.

The consolidation of data centers through virtualization has been on the agenda for many years, and many players have come far in working towards a solution. A few have gone further and helped IT operations benefit from Enterprise-wide use of Cloud, serving most of the organization’s applications, such as customer relationship management and billing. The journey must entail process, people and technology dimensions to successfully deploy cloud, serving both legacy and new processes and applications.

Through management and orchestration, as well as service enablement functions, it is possible to adapt network functions easily and flexibly, in order to meet the diverse and personalized needs of the market.

NETWORKS:

In the operator telecom cloud, transformation with new virtualized network functions enables speed, efficiency and service innovation. Examples of such virtualized functions are Evolved Packet Core (EPC) and IMS. Also in the radio access domain, virtualization is happening. For example, functions can be moved to the edge of the mobile network to improve coordination of radio features and allow for deployment of other functionality that normally resides higher up in the network, e.g. IoT functions.

MEDIA

The adoption of distributed and flexible computational platforms for all forms of data manipulation and hosting has become the norm in many industries. In TV and Media, this philosophical approach is being applied to many if not all aspects of processing

functions that span metadata, user interfaces, management and video-specific processing.

Virtualization approaches using Cloud technology will underpin the majority of Media processes and business platforms to deliver the agility in experiences, efficiency of operations and infrastructure, enable the transition to software-defined workflows, processing and business models.

Cloud-based offerings within media are:

- Cloud Digital Video Recorders – removing the physical barriers to access recorded content when not at home
- Cloud-enabled Media Management – services designed to manage secure contribution, archiving and media processing in the public and private cloud
- Media/ TV platform – bringing the agility, innovation and economic benefits of modern cloud technologies and web services to Pay TV operators

INDUSTRIES

- Connected Vehicle Cloud – connects vehicles and their occupants with services and information from various service and content providers, including the automotive manufacturer
- Maritime ICT Cloud – connects vessels at sea with shore-based operations and service providers to, for example, manage fleets, monitor engines and fuel consumption, oversee routes and navigation, integrates documentation and information flows into port operations, and ensure the wellbeing of crew.
- Connected traffic cloud – supports road authorities to have improved visibility of traffic conditions by integrating data from authority's own sources as well as from connected cars, internet feeds and potentially other sources, and allows more precise communication to drivers via timely and relevant information delivery into cars.

We therefore urge Telecom Regulatory Authority of India to consider having a light touch regulation on Cloud and Cloud based technologies (both private and public) to facilitate innovation, cost-optimization (both capex and opex), economies of scale in operations, lower cost of delivery to consumers by enterprises, low tariffs for end-consumers and more importantly to expedite IOT based applications in over 50 billion connected devices world in near future.

Sincerely yours

For Ericsson India Pvt. Limited

SREENIVASA REDDY
Director - Corporate Affairs & Industry Relations

Question 1:

What are the paradigms of cost benefit analysis especially in terms of –

a. **accelerating the design and roll out of services**
b. **Promotion of social networking, participative governance and e-commerce.**
c. **Expansion of new services.**
d. **Any other items or technologies. Please support your views with relevant data.**

Response:

a) Any service implementation entails three fundamental building blocks – compute, storage and connectivity. In the case of traditional service architecture which utilized standalone monolith boxes, this entailed planning the precise location of points-of-presence (PoPs) & infrastructure, flawlessly. Since elasticity is not there in such traditional architectures, infrastructure is rather over-provisioned to overcome intermittent surges and future scaling. As a result, it is complex to operate such infrastructure and also capex is very high.

On the contrary, Cloud technology provides flexible on-demand elastic capacity, API's framework and readily available run-time environment with on-the-go provisioning and pay-per-use facility in self-service manner. Secondly the cloud computing paradigm offers global footprint almost on instantaneous basis.

Cloud services provide infrastructure, platform and software-as-a-service (SaaS). As a result, anyone including amateurs, developer community and enterprises could design and implement services leveraging offered API's and utilizing service catalogue feature in the cloud manager in an instant manner. Of course, while subscribing a cloud service, one needs to take care of the API's and run-time environment needed besides the specifics of the platform which a customer would require.

b) Social networking is an application which is highly storage intensive and demanding large footprint with uniformity of experience. Leveraging Cloud based technology in social networking is widely proven. The global scale and elasticity which is provided by clouds allows quick scaling and global presence to all citizens across nations who have access to internet (or intranet in case of a private cloud). Any application including interactive eGov. etc. can be launched in a similar manner across the nation.

In fact, we would be happy to suggest a vision that all citizen services forming part of eGov. to be hosted on a government cloud – public safety, financial inclusion, health and emergency communication etc. This cloud could also be used to cater all government users.

c) Owing to standard API's framework, new services could be quickly designed using the standard API's and developers can also develop their API's from scratch using the runtime environment, object libraries offered by cloud service provider.

Question 2. Please indicate with details how the economies of scale in the cloud will help cost reduction in the IT budget of an organization?

Response:

Cloud computing enables IT and provides both management and technical experts, an instant access to compute & storage resources accelerating innovations – both from development and go-to-market (GTM) perspective.

Operational efficiencies can be achieved in two ways: lower infrastructure costs and increase efficiency of the team. The former is possible by accessing lower cost compute resources & controlling excess capacity while latter is possible by leveraging automation and self-service.

- aspects such as charging on pay-per-use charging can significantly reduce the costs for variable workloads
- self-service can reduce the workload on help-desks.

- Global footprints can be expanded by using the public clouds – that have the ability to offer services and products in open markets – globally.

- Economies of scale in cloud can help in cost reduction, 100% hardware utilization and making the whole cloud ecosystem greener.

- *Lower Costs*

  - **Configuration and manpower** – Traditional architectures includes scattered router, switches and firewalls across geographies. Tremendous complexity in VLANs/ IP's etc. for creating an interconnection topology is involved which creates still greater challenge when expansion is called for or there is a change in the geographical location of infrastructure. With automation on this front possible in cloud supported by NFV and SDN, this humongous configuration load is eliminated thereby saving precious time, efforts and costs.

- ***Green ICT -*** Lesser infrastructure and power consumption leads to sustainability and reduce carbon footprint.

We would like to bring to your kind notice about the outcome of a research conducted by Mainstay LLC in USA (www.mainstaycompany.com), on the economics of disaggregated hyperscale data center based on OpenStack, having both electrical and optical interface.

Question 3. What parameters do the business enterprises focus on while selecting type of cloud service deployment model? How does a decision on such parameters differ for large business setups and SMEs?

Response:

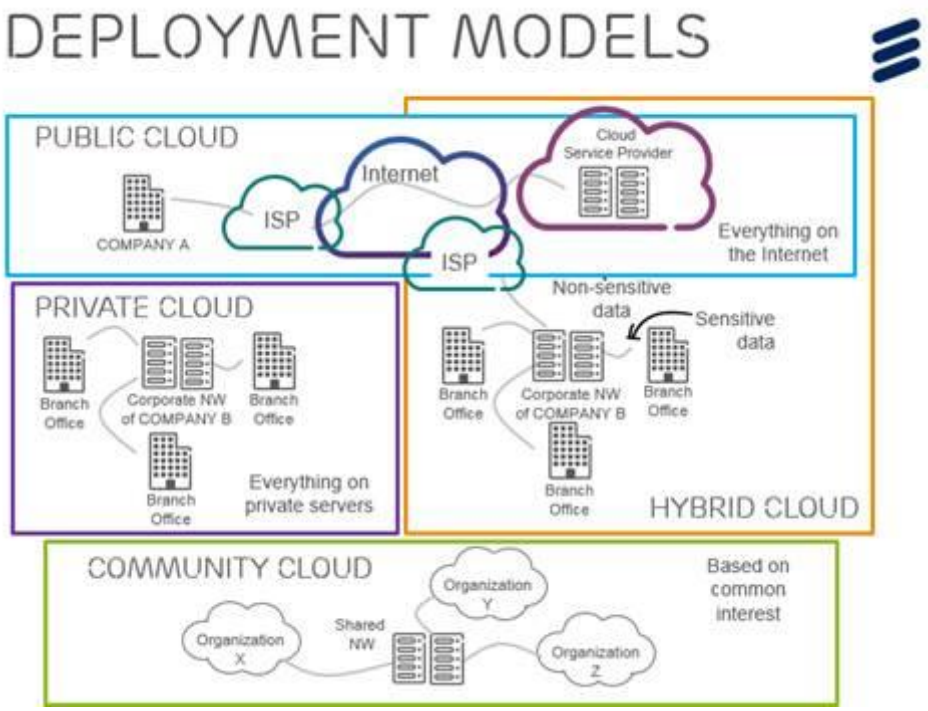
The NIST definition defines four deployment models:

Public Cloud: In simple terms, public cloud services are characterized as being available to clients from a third party service provider via the Internet. The term “public” does not always mean free, even though it can be free or fairly inexpensive to use. A public cloud does not mean that a user’s data is publically visible; public cloud vendors typically provide an access control mechanism for their users. Public clouds provide an elastic, cost effective means to deploy solutions.

Private Cloud: A private cloud offers many of the benefits of a public cloud computing environment, such as being elastic and service based. The difference between a private cloud and a public cloud is that in a private cloud-based service, data and processes are managed within the organization without the restrictions of network bandwidth, security exposures and legal requirements that using public cloud services might entail. In addition, private cloud services offer the provider and the user greater control of the cloud infrastructure, improving security and resiliency because user access and the networks used are restricted and designated.

Community Cloud: A community cloud is controlled and used by a group of organizations that have shared interests, such as specific security requirements or a common mission. The members of the community share access to the data and applications in the cloud.

Hybrid Cloud: A hybrid cloud is a combination of a public and private cloud that interoperates. In this model users typically outsource non business-critical information and processing to the public cloud, while keeping business-critical services and data in their control. A way of utilizing public cloud infrastructure in a private or semi-private manner and interconnecting these resources to the internal resources of a consumers’ datacentre, usually via virtual private network (VPN) connectivity.



There are a few parameters that can be used when evaluating the cloud services deployment model. Not all the parameters will be used for any one enterprise.

- API framework
- Runtime environment
- Data privacy and security requirements
- Openness of the platform
- Performance levels
  - SLA & SLP
  - Operational Transparency
  - Multi-tenancy
- Cost (Capex and Opex)
- Reliability
  - Disaster recovery plan
- Network Scalability and Security
- Cloud Management
  - Control
  - Integration
  - Inter-Operability
  - Transition/ Migration (one cloud to another)
- Big Data (Volume, Velocity, Variety and Veracity)

Question 4. How can a secure migration path may be prescribed so that migration and deployment from one cloud to another is facilitated without any glitches?

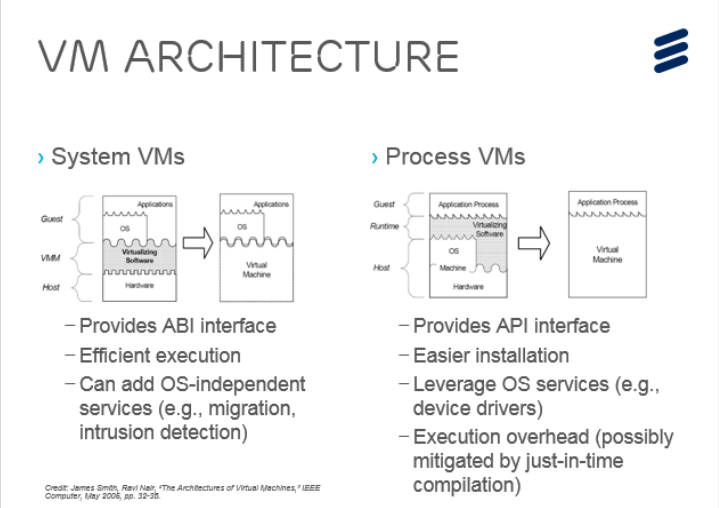
Response:

Cloud portability refers to the ability to move cloud applications from one cloud to another which reduces vendor lock-in problem. Interoperability is fundamental enabler for exchange of information across organizations and cloud environments.

Cloud providers do provide mechanisms to support data portability, service interoperability, and system portability. Data portability is the ability of cloud consumers to copy data objects into or out of a cloud or to use a disk for bulk data transfer.

Service interoperability is the ability of cloud consumers to use their data and services across multiple cloud providers with a unified management interface. System portability allows the migration of a fully-stopped virtual machine instance or a machine image from one provider to another provider, or migrate applications and services and their contents from one service provider to another. It may be noted that various cloud service models may have different requirements in relation with portability and interoperability. For example, IaaS requires the ability to migrate the data and run the applications on a new cloud.

Thus, it is necessary to capture virtual machine (VM) images and migrate to new cloud providers which may use different virtualization technologies. Any provider-specific extensions to the VM images need to be removed or recorded upon being ported. While for SaaS, the focus is on data portability, and thus it is essential to perform data extractions and backups in a standard format. The following requirements are related to portability and interoperability for secure migration: Service entities (for example, VMs) should be able to migrate across organizational and ownership boundaries (for example, between an enterprise and a service provider's IaaS infrastructure). In the case of a virtualized infrastructure, VM migration should address secure deprovisioning (removal of the VM image after it is ported to a different location or service provider) and partial migration (cloud burst: secure integration between old and new locations and service providers). Service providers shall provide assurance on the consistency of control effectiveness, management, monitoring, and reporting interfaces and their integration across old and new locations and providers.



If storage migration capabilities are provided, the service provider should have verified functionalities for secure data transfer including encryption, access control, key management, decommissioning of storage devices, and destruction of data after migration.

Migration of cloud applications:

Challenges in migration:
Moving applications to the cloud may not be that easy. All applications may not be suitable for deployment to cloud based solutions. This can result in compatibility issues for application installation and running, update and un-installation processes leading to the following problems:

1. OS platform assessment and remediation
2. Virtualization platform assessment
3. Application conversion to target platform
4. Middleware and dependency management
5. User state and profile management

Question 5. What regulatory provisions may be mandated so that a customer is able to have control over his data while moving it in and out of the cloud?

Response:

Ericsson requests TRAI in general to consider the OECD 2013 privacy guidelines (http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm) related to international transfers as below:

- A data controller remains responsible for personal data under its control without regard to the location of the data.
- A country should refrain from restricting trans-border flows of personal data between itself and another country where:

  - the other country substantially observes the OECD guidelines or
  - Sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with OECD guidelines.

- Any restrictions to trans-border flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

- Mutual Legal Assistance Treaties are a key tool for addressing law enforcement access to commercial data that can reduce unnecessary and disproportionate burdens on commercial entities by enhancing the effectiveness and interoperability of cross-border or extraterritorial lawful access to personal data by enforcement agencies.

Key Policy Considerations:

- Policy makers should strive to achieve a liberal and simplified (minimizing administration/red tape) regulation of trans-border flows of personal data in the spirit of free trade. We believe that this can be achieved while, at the same time, maintaining an adequate level of protection of personal data and privacy. As a principle restrictions and prohibitions of cross-border transfers of personal data for legitimate commercial processing purposes should be kept to a minimum.

- Policy makers should promote and expand international harmonization, such as mutual recognition or adequacy assessments of nations' privacy regulation with the aim to abolish the need for a competent authority to approve cross-border data flows or the need for controllers or processors to rely on specific legal transfer mechanisms.

- When international harmonization of national privacy regulation cannot be realistically achieved, or is expected to take a long time, policy makers should foster the introduction of legal transfer mechanisms similar to the U.S. Safe-Harbor Company certification or the EU Binding Corporate Rules (for controllers and processors) or EU Standard Contractual Clauses to handle different levels of stringency in national data protection or other relevant privacy laws, to facilitate trans-border data flows.

- Where such legal transfer mechanisms are available, additional approvals by a national competent authority should not be required for cross-border data transfers already covered by the legal transfer mechanisms.

- Where such legal transfer mechanisms are not-available and harmonization has not been achieved, policy makers should strive to minimize cross-border data transfer administrative burdens and institute effective and predictable cross-border data transfer approval processes, e.g. setting maximum approval lead times, preferably to less than 30 days.

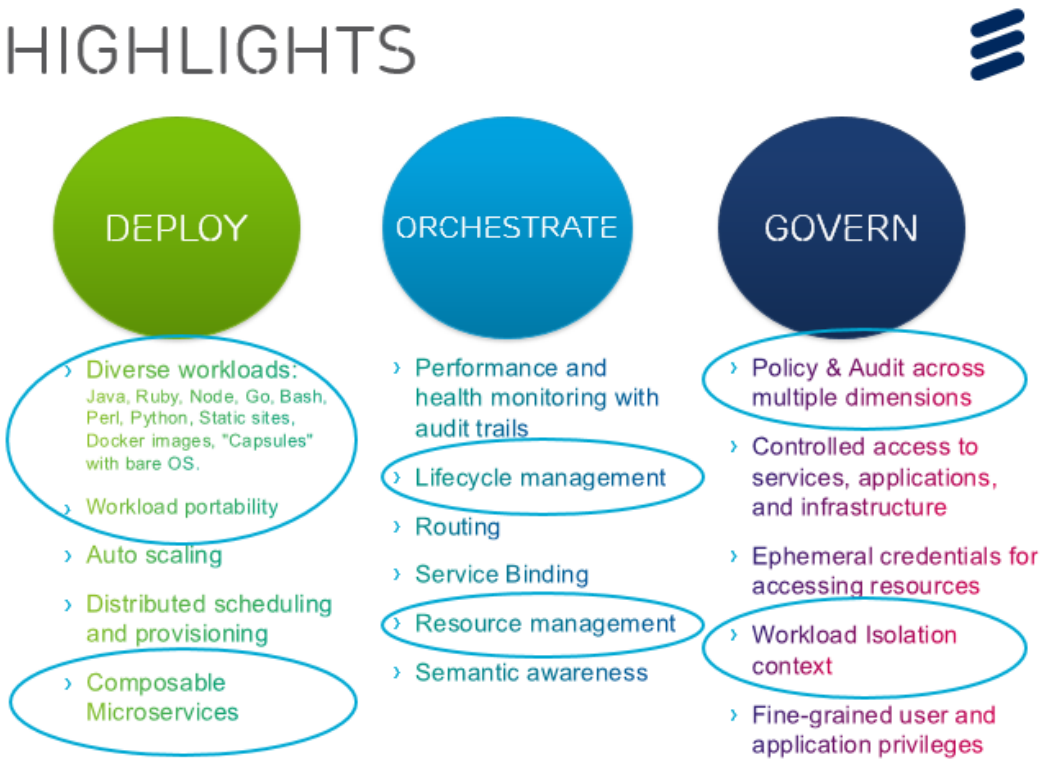
Question 6. What regulatory framework and standards should be put in place for ensuring interoperability of cloud services at various levels of implementation viz. abstraction, programming and orchestration layer?

Response:

The U.S. National Institute of Standards and Technology (**NIST**) defined that, cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

These unique capabilities brought to bear to offer global cloud infrastructure network



Service providers needs consistent security management system wide. The end user needs trusted storage and networking in the cloud.

Centralized management which includes the Identity and access management, IdAM and Security and audit trail logging access. For the End user security, there is Traffic separation, providing tenant and user isolation as well as Secure interface to cloud management.

1. Identity and Access Management - authentication & access control services, …
2. Key and Certificate Management - security protocols, encryption, …
3. Network Security - firewall, antivirus, isolation, …
4. Security Analytics - monitoring, analysis, detection, protection, visualization, …

Also, *Active/active HA with loadsharing t*o ensure continuous access to service; ensure redundant key components, better monitoring and fault handling, and reduced churn through increased user experience

Mobile connectivity has been able to scale at this pace due to the industry focus on global standards, interoperability and other factors. Network Functions Virtualization (NFV) platform provides interoperability and connectivity with any carrier class virtualized network function and SDN.

Question 7. What shall be the QoS parameters based on which the performance of different cloud service providers could be measured for different service models? The parameters essential and desirable and their respective benchmarks may be suggested.

Response:

The metrics above are generally defined in terms of machine characteristics; better performance metrics tend to be defined in terms of application performance. We discuss some of these below.

Program Execution Time:

This metric is defined by the elapsed wall clock time from program start to finish. Some professionals consider this to be the only meaningful and informative metric and suggest that any other metric may be misleading. Performance has a direct relationship with execution time which means faster execution times give higher performance scores.

Throughput:

Throughput (CPU bandwidth) is defined as the number of units of work per unit time (usually per second) the CPU can perform. For consistency, the unit of work should be well defined and remain constant. As discussed there is no commonly accepted definition of unit of work, and so this becomes workload dependent.

Work done in a fixed time:

In the program execution time metric, the amount of work done is fixed and wall clock time is the variable of interest. Users prefer to purchase cloud services that allow more work to be done in the same amount of time when compared to older systems.

By ‘more work’ they tend to mean solving a larger problem, not just an increase in throughput. This could be, for example, running a Monte Carlo Simulation at a much greater number of iterations to produce smaller error bounds on estimates.

Response Time:

The above metrics are suitable for batch jobs. For interactive applications or websites, response time (also known as application latency) is a good metric. It may be shown that higher response times lead to lower user satisfaction. In general, the good metrics relate to application performance and not machine characteristics. Given this, ratings that relate equivalent performance to specified physical machines, as currently favored by large Cloud providers, are unsatisfactory for most purposes. And, as we will show, these are also not particularly meaningful even for comparing virtual machines in the same Cloud (provider). Cloud Service Brokerages, then, would add good value by selecting good performance metrics that can clearly relate to the applications that their customers wish to run.

There are several distinct options provided by Cloud vendors dealing with the IT needs of multiple companies. Each decision has got very different efficiency regarding performance, service latency and precision. Institutions ought to recognize how their programs can do on the numerous Clouds and also whether or not those deployments satisfy their goals. Performance means diverse things in many contexts. Generally, it's relevant to response time (the time it requires to process a demand), throughput (how much number of requires over-all might be done per unit of the time), or even timeliness (capability to meet deadlines, i.e. to process requesting in a settled and appropriate time period).

Question 8. What provisions are required in order to facilitate billing and metering re-verification by the client of Cloud services? In case of any dispute, how is it proposed to be addressed/ resolved?

Response:

The cloud billing system needs to take into its stride all forms of cloud products and services provided by the cloud service provider. It needs to be scalable and responsive to demands. It needs to furnish data to users in real-time and should be able to display up-to-date changes in cloud computing services enjoyed by a consumer. Last but not the least, a cloud billing system has to be transparent and customer-facing such that consumers are always kept informed on the resources being used or have been used, and the billed and/or payable amounts in respect thereof.

The “pay-as-you-go”, the “pay-for-resources”, and prepayment of charges are available for cloud services. Foremost is the issues related to integrity of billing transactions and monitoring Service Level Agreement parameters at all times.

The cloud charging and billing model is a complex framework since there are different layers of service offerings – SaaS, PaaS and IaaS. Depending on the layer subscribed there are going to be different billing models. Cloud service provider infrastructure needs to have capability to produce records on resource utilization to reconcile on extent of usage, example: compute or storage resource utilization versus installed capacity.

The manner in which service requests could be charged is determined by the Pricing mechanism. Not all requests can or should be treated equally. Pricing requests, therefore, need to be considered in the light of peak and off-peak basis, and on the availability of demand to supply ratios.

Cloud provider needs maintaining a record of resource-consuming activities on account of any given user. Records maintained through this mechanism can be collated and computed with respect to Pricing mechanism, and a final charge statement can then be presented to the consumers.

Question 10. Enumerate in detail with justification, the provisions that need to be put in place to ensure that the cloud services being offered are secure.

Response:

To run a trusted cloud business, an organization utilizing cloud-based services requires trusted operations, trusted networks and trusted products enabling trusted services.

Several organizations, for example, the European Network and Information Security Agency and the Cloud Security Alliance, have studied the security challenges of cloud computing and have found them to culminate in the following three basic challenges:

Multi-tenancy – Resources are shared between tenants according to Service Level Agreements (SLAs). Each provider is responsible for a proper isolation of its tenants' computing, networking and storage resources.

Divided responsibility – Besides the provider, tenants also have the responsibility to protect their assets. Dividing responsibility between the provider and the tenant depends on the SLA, and needs to be agreed between the actors before the service is taken in use.

Dynamic environment – The cloud environment is constantly evolving, and resources may dynamically scale up and down or even change their locations. Security policies have to capture and govern these dynamic changes.

To counteract these challenges, it is important for the tenant to be able to verify that services are available and that they are protected according to a desired or agreed-upon policy and SLAs.

The challenges also imply the importance of data protection. Data needs to be available, its integrity protected and the confidentiality of sensitive data assured. For example, multi-tenancy must not disclose data to unauthorized tenants, nor cause deviation from the desired level of data availability. Confidentiality and integrity of data cannot be lost due to divided responsibility between actors. The integrity of security policies should not be broken because of dynamic changes in the service deployment.

The previously mentioned security challenges generate an obvious need for advanced risk and threat management. In the current business environment, each cloud service provider needs relevant and efficient measures for turning cybersecurity from an uncontrollable extra cost into an efficiently managed competitive advantage. To run a trusted cloud business, an organization utilizing cloud-based services requires trusted operations, trusted networks and trusted products enabling trusted services.

For details kindly refer to Ericsson's paper:
https://www.ericsson.com/res/docs/whitepapers/wp-cloud-security.pdf

Question 12. What security provisions are needed for live migration to cloud and for migration from one cloud service provider to another?

Response:

Various Techniques that are used for VM (Live) Migration-

A. **Energy Efficient Migration Technique**: The maximum power consumed by any server is up to 70%, even at their highest utilization level

B. **Load Balancing Migration Technique**: Migration technique can be used to distribute load across the servers in order to improve the scalability of cloud environment. It helps in minimizing the resource consumption; avoid bottlenecks and overprovisioning of resources.

C. **Fault tolerant Migration Technique:** If any part of the system fails then the fault tolerant migration technique can be used to keep the application running. This technique transfers the application from the failed VM to other VM and it is based upon future prediction of the system.

Security Concerns in Migration:

- The attacker may steal the bandwidth by taking the control of source virtual machine and migrating it to the destination virtual machine.

- The attacker may falsely advertise its resource and attract others to migrate its resources towards itself.
- Passive snooping: Attacker just accesses the data of migration using any sniffing tool that may lead to leakage of some confidential information.
- Active manipulation: Attacker may modify the data which is travelling from the source to the destination.

---------- End of Document ----------